**THE UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF TEXAS**
**DALLAS DIVISION**

| | |
|---|---|
| **JEFF M EDWARDS, individually,** | **CASE NO. 3:24-CV-02543-E** |
| **Plaintiff** | |
| **vs.** | **MDL CASE NO. 3:24-MD-03114** |
| **AT&T, INC.** | **PLAINTIFF'S AMENDED COMPLAINT** |
| **Defendant** | |

**Plaintiff Jeff M Edwards ("Plaintiff") brings this "Amended Complaint" against the Defendant, AT&T, Inc. ("Defendant" or "AT&T") and hereby alleges, upon personal knowledge as to his own action and investigation, and upon information and belief as to all other matters, asserts the following claims before the Court.**

**Plaintiff's "Original Complaint", pursuant to Texas Government Code 27.031(a)(1), limited Plaintiff's damages. Conversely, Defendant's actions were in direct violation of Texas Business and Commerce Code - Sec. 521.052, namely, "BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION",**

> **(a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.**

**By Defendant's admission (Exhibit A) in its "Notice of Data Breach", Defendant states; *"What information was involved? The information varied by individual and account, but may have included full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and AT&T passcode."***

**F-Secure, a global cybersecurity company that offers products and services to protect consumers from online threats, confirmed (Exhibit B) that Plaintiff's social security number, along with other personal information (PI) was not only exposed but stolen with Defendant's own AT&T Data Breach.**

**Pursuant to Rule 15(a) of the Federal Rules of Civil Procedure, Plaintiff, "as a matter of justice", submits to the Court "Plaintiff's Amended Complaint".**

## PARTIES

**1. Plaintiff Jeff M Edwards is a Texas citizen who lives in Cedar Park, Texas. Plaintiff's principal address at all times pertaining to this action is 1406 Duster Cove, Cedar Park, Texas, 78613. Plaintiff is a former customer of AT&T Inc. having received internet as well as other telecommunications services from Defendant.**

**2. AT&T Inc. (with "AT&T" being an abbreviation for its former name, the American Telephone and Telegraph Company) is a multinational telecommunications company. It is the world's fourth-largest telecommunications company by revenue and the largest wireless carrier in the United States. As of 2023, AT&T was ranked 13th on the Fortune 500 rankings of the largest United States corporations, with revenues exceeding $100 billion.**

**AT&T provides, among other things, wireless network services, cellular data plans, cell phone plans, and Internet connection plans.**

**3. Defendant AT&T, Inc. (Defendant) is headquartered at 208 South Akard Street, Dallas, Texas 75202, and may be served through their registered agent CT Corporation System, 1999 Bryan Street., Ste. 900, Dallas, Texas 75201.**

## JURISDICTION AND VENUE

**4. On June 18, 2024, Plaintiff filed an "Original Complaint" against the Defendant in Williamson County, Texas Justice Court. Subsequently, the Defendant filed a "Notice of Removal" to the United States District Court for The Western District of Texas. Thereafter, Plaintiff filed an objection.**

**5. On October 4, 2024, the United States District Panel on Multi-District Litigation granted a transfer order (Exhibit C) under case number 3:24-cv-02543-E moving this action to the United States District Court for The Northern District of Texas as part of MDL case number 3:24-md-03114.**

**6. The Panel found:** ***After considering the argument of counsel, we find that the actions involve common questions of fact with the actions transferred to MDL No. 3114, and that transfer under 28 U.S.C. § 1407 will serve the convenience of the parties and witnesses and promote the just and efficient conduct of the litigation. In our order establishing this MDL, we held that centralization was warranted for actions concerning "an alleged data security breach announced by AT&T in March 2024 concerning the personal information of over 70 million former and current AT&T customers released on the dark web."2 See In re AT&T Inc. Customer Data Sec. Breach Litig., __ F. Supp. 3d __, 2024 WL 2884429 (J.P.M.L. June 5, 2024). The actions concern the AT&T data breach announced in March 2024 and share common factual questions with the actions in the MDL.***

**7. This action is brought pursuant to Texas Business and Commerce Code - BUS & COM Sec. 17.565 and Sec. 521.052.**

**8. The United States District Panel on Multi-District Litigation, by its transfer order of October 4, 2024 (Exhibit C), has deemed the United States District Court for The Northern District of Texas as part of MDL case number 3:24-md-03114 as the proper court having jurisdiction and the proper venue for this action.**

## DEFENDANT'S NOTICE TO PLAINTIFF

**9. On April 25, 2024, Defendant AT&T sent a formal notice of a "Data Breach" to Plaintiff Jeff M Edwards with the subject heading "Notice of Data Breach" (Exhibit A).**

**10. With the above notification, Defendant AT&T has acknowledged the Data Breach and has admitted this serious error.**

## CASE BACKGROUND

**11. This action arises out of a recent targeted cyberattack and data breach ("Data Breach") in which Defendant AT&T, lost control over more than 73 million customers' personal data and other sensitive information. Those customers, including Plaintiff, suffered ascertainable losses from this Data Breach including the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, now and into the future.**

**12. Plaintiff Jeff M Edwards' personal data and other sensitive information, including Plaintiff's social security number, which was entrusted to Defendant for safe keeping—was compromised and unlawfully accessed due to the Data Breach.**

**13. The Data Breach included personally identifiable information ("PII") that Defendant collected and maintained. Information compromised in the Data Breach includes, names, addresses, phone numbers, dates of birth, Social Security Numbers, and email addresses ("Private Information").**

**14. Plaintiff brings this lawsuit to address Defendant's inadequate safeguarding of Plaintiff's Private Information that it collected, and for failing to provide timely and adequate notice to Plaintiff that his information had been subject to the unauthorized access of unknown third parties and precisely what specific type of information was**

accessed.

15. Defendant collected and stored Plaintiff's Private Information in a reckless manner.

16. In particular, Private Information was collected by Defendant, inadequately secured, and shared with a vendor who had insufficient cybersecurity protections in place to protect Plaintiff's Private Information.

17. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

18. Plaintiff's identity is now at increased risk of identity theft because of Defendant's negligent conduct since the Private Information that Defendant collected and promised to protect is now in the hands of data thieves.

19. The seriousness and gravity of Defendant's Data Breach, especially the fact that Plaintiff's Social Security number was exposed to thieves and, therefore, stolen, the Social Security Administration (Exhibit D) states;

"Identity theft is one of the fastest growing crimes in America. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems."

20. Armed with the Private Information accessed in the Data Breach, data thieves can now commit a variety of crimes including, e.g., opening new financial accounts in Plaintiff's name, taking out loans in his name, using Plaintiff's information to obtain government benefits, filing fraudulent tax returns using Plaintiff's information, obtaining driver's

licenses in Plaintiff's name, but with another person's photograph, and giving false information to police during an arrest.

21. As a result of the Data Breach, Plaintiff has been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff must now and in the future closely monitor his financial accounts to guard against identity theft.

22. Plaintiff is also very likely to incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

23. Plaintiff seeks to remedy these harms as a result of the Data Breach caused by AT&T.

24. Plaintiff seeks remedies including, but not limited to, compensatory and exemplary damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security protocols, future annual audits, and adequate credit monitoring services funded by Defendant.

## NATURE OF DEFENDANT'S BUSINESS

25. Defendant AT&T is a company that provides telecommunications services across the United States.

26. In the ordinary course of providing telecommunications services, customers must provide to AT&T access to certain Private Information. AT&T specifies the following types of personal data collected in its "Privacy Notice: The information we collect".

To better run our business, we collect information about you, your equipment and how you use our products and services. This can include:

a. Account information. You give us information about yourself, such as contact and

**billing information. We also keep service-related history and details, including Customer Proprietary Network Information.**

**b. Equipment information. We collect information about equipment on our network**

**c. like the type of device you use, device ID, and phone number.**

**d. Network performance. We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working.**

**e. Location information. Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites.**

**f. Web browsing and app information. We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information.**

**g. Biometric information. Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice.**

**h. Third-party information. We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and**

**geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.**

**All these types of information are considered Personal Information when they can reasonably be linked to you as an identifiable person or household. For instance, information is personal when it can be linked to your name, account number or device.**

**27. Within AT&T's Privacy Notice, AT&T states the following about keeping Private Information private and secure:**

***"Thank you for reading our Privacy Notice. Your privacy is important to you and to us. This notice applies to AT&T products and services including internet, wireless, voice and AT&T apps. Your privacy choices and controls You can manage how we use and share your information for certain activities including advertising and marketing. Here are key examples: Do not sell or share my personal information. We may share information with other companies in limited ways, such as exchanging subscriber lists for joint marketing. Data retention and security. We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information. No security measures are perfect. We can't guarantee that your information will never be disclosed in a manner inconsistent with this notice. If a breach occurs, we'll notify you as required by law".***

**28. Thus, because of the highly sensitive and personal nature of the information it acquires, AT&T promises in its Privacy Notice to, among other things, maintain the privacy and security of Private Information.**

**29. As a condition of receiving telecommunications services, Defendant requires that its customers entrust it with highly sensitive personal information.**

**30. By obtaining, collecting, using, and deriving a benefit from Plaintiff' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff' Private Information from disclosure.**

**31. Plaintiff have taken reasonable steps to maintain the confidentiality of their Private Information.**

**32. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.**

## THE "DATA BREACH"

### A. 2021 Stealing of Database ("2021 Data Incident")

**33. On or about August 19, 2021, a criminal hacking group called "ShinyHunters" began selling on a hacking forum a database which, according to ShinyHunters, contains Personal Customer Data of over 70 million AT&T customers.**

**34. While attempting to sell the database, ShinyHunters only revealed sample data from the compromised database, which included customers' names, addresses, phone numbers, Social Security numbers, and dates of birth.**

**35. AT&T maintained, without providing any evidence, that the data samples leaked from the compromised database did not come from AT&T's systems, that AT&T had**

not been breached.

36. AT&T also did not confirm whether the leaked data came from a breach of a third-party partner's information technology systems which may have held Private Information.

37. ShinyHunters challenged AT&T's denials of the Data Breach coming from AT&T or one of its third-party partners, stating "I don't care if they don't admit. I'm just selling."

38. ShinyHunters also stated that the criminal group was willing to "negotiate" with AT&T.

39. Shortly after the 2021 Data Incident, a security researcher reported that two of the four individuals in the data samples leaked by ShinyHunters were confirmed to have accounts on att.com.

40. AT&T did not notify any of its customers, including Plaintiff, of the 2021 Data Incident. Defendant's actions, therefore, are serious and in direct violation of Texas Business and Commerce Code - Sec. 521.052

B. 2024 Leak of Private Information ("2024 Data Incident")

41. On or about March 17, 2024, another cybercrime actor known as "MajorNelson" posted on an Internet forum the entire dataset of the stolen database from the 2021 Data Incident, the database of which ShinyHunters attempted to sell.

42. The data leaked by MajorNelson included the following data types from approximately 73 million individuals, inter alia: names, addresses, phone numbers, dates of birth, and Social Security numbers.

43. On March 19, 2024, Troy Hunt—a security researcher and the creator of the data breach notification website "Have I Been Pawned"—posted on his blog about the AT&T

**Data Breach.**

**44. In the blog post, Mr. Hunt concluded that the leaked data from the Data Breach was authentic after he spoke with several "Have I Been Pawned" subscribers who were AT&T customers and who confirmed the accuracy of the leaked data.**

**45. Moreover, Mr. Hunt noted that the Internet forum on which the leaked data was posted is not on the 'dark web,' but rather on the traditional Web "easily accessed by a normal web browser."**

**46. The 2021 Data Incident combined with the 2024 Data Incident (together, the "Data Breach") caused significant harm to Plaintiff.**

### C. AT&T Failed to Safeguard Plaintiff's Private Information

**47. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff to keep his Private Information confidential and to protect it from unauthorized access and disclosure.**

**48. Plaintiff provided his Private Information to AT&T with the reasonable expectation and mutual understanding that Private Information would comply with Defendant's obligation to keep such information confidential and secure from unauthorized access.**

**49. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the breach.**

**50. In light of recent high profile data breaches at other companies, Defendant knew or should have known that electronic records would be targeted by cybercriminals.**

**51. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like**

**smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."**

**52. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.**

**53. AT&T failed to implement adequate data security measures to safeguard Plaintiff's Private Information as evidenced by the database stolen by ShinyHunters in 2021 and by the full leak of about 73 million individuals' Private Information by MajorNelson in 2024, nearly three years after the 2021 Data Incident.**

**54. Despite the First Data Incident having occurred in August 2021 (and again on March 2024), AT&T has made no effort to notify the public about the severity of the Data Breach nor has AT&T given to potential victims of the Data Breach instructions on how to keep their Private Information safe.**

**55. Even though the Private Information at issue has been compromised and leaked for about two and a half years, AT&T has done nothing to get the leaked Private Information taken down from places where the Private Information should not be, such as in the aforementioned internet forum, which are on the Clear Web.**

**56. Further, AT&T has not done anything to determine the source of the Data Breach. This is evidenced by AT&T's reluctance to confirm whether the Data Breach may be attributed to a third-party partner to whom AT&T entrusted the processing and safekeeping of a substantial amount of Plaintiff' Private Information.**

**57. Considering that the Data Breach likely occurred as a result of malicious actors—such as ShinyHunter and MajorNelson—exploiting a data security weakness in one of**

**AT&T's third-party processors of Private Information, AT&T failed to adequately verify the adequacy of security measures, if any, that such third-party processors had in place meant to protect the Private Information.**

**D. Defendant Failed to Comply with FTC Guidelines**

**54. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.**

**55. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.***

**56. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.**

**57. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.**

**58. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information is an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.**

**59. Defendant was at all times fully aware of its obligation to protect the Private Information of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.**

**E. Defendant Failed to Comply with Industry Standards**

**60. As shown above, experts studying cyber security routinely identify companies as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.**

**61. Several best practices have been identified that a minimum should be implemented by companies like Defendant, including but not limited to ensuring Private Information is only shared with third parties when reasonably necessary and that those vendors have appropriate cybersecurity systems and protocols in place.**

**62. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards. The**

**Center for Internet Security ("CIS") released its Critical Security Controls ("CSC"), and all businesses are strongly advised to follow these actions. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.18**

**63. Other best cybersecurity practices that are standard in the telecommunications industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.**

**F. Cyberattacks and Data Breaches Put Individuals at an Increased Risk of Fraud and Identity Theft**

**64. Cyberattacks and data breaches on businesses are problematic because of the increased risk of fraud and identity theft. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face *"substantial costs and time to repair the damage to their good name and credit record."* That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate**

**pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.**

**65. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.**

**66. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.**

**67. Identity thieves can use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. Also, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.**

**68. Moreover, theft of Private Information is also gravely serious. PII is a valuable property right. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.**

**69. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information is stolen and when it is used.**

**70. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. See GAO Report, at p. 29.**

**71. Private Information is such a valuable commodity to identity thieves that once the information has been compromised criminals often trade the information on the "cyber black market" for years.**

**72. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning *Plaintiff is at an increased risk of fraud and identity theft for many years into the future.***

**73. Thus, Plaintiff must vigilantly monitor his financial accounts and other types of accounts for many years to come.**

**74. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.**

**75. For example, the Social Security Administration (Exhibit D) has warned that identity thieves can use an individual's Social Security number to apply for additional**

**credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.**

**76. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."**

**77. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, *"[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."***

**78. Because of the value of its collected and stored data, the telecommunications industry has experienced disproportionally higher numbers of data theft events than other industries.**

**79. For this reason, Defendant knew or should have known about these dangers and strengthened its data protocols accordingly. Defendant was put on notice of the substantial**

and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

## CLAIMS FOR RELIEF

### COUNT I: NEGLIGENCE

80. Plaintiff repeats and re-alleges each and every factual allegation contained in each and every previous paragraph as if fully set forth herein respecting this, "Plaintiff's Amended Complaint".

81. In order to receive telecommunications services, Defendant required Plaintiff to submit non-public Private Information, such as PII.

82. Plaintiff entrusted his Private Information to Defendant with the understanding that Defendant would safeguard his personal information as required by Texas law.

83. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property to prevent disclosure of the information, and to safeguard Plaintiff's personal information (PII) from theft.

84. Defendant's duty included a responsibility to fully vet vendors with whom it shared Private Information and ensure that those vendors had adequate data security protocols and procedures in place.

85. Defendant owed a nondelegable duty of care to Plaintiff to provide proper and adequate data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

**86. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff from a data breach.**

**87. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.**

**88. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the law described above, but also because Defendant is bound by industry standards to protect confidential Private Information.**

**89. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures in its own systems to protect Plaintiff's Private Information and by failing to properly verify that its third-party processors implemented data security measures adequate to safeguard Plaintiff's Private Information.**

**90. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the telecommunications industry.**

**91. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's Private Information would result in one or more types of injuries to Plaintiff.**

**92. Plaintiff is, therefore, entitled to compensatory, consequential and exemplary damages suffered as a result of the "Data Breach".**

**93. Plaintiff is also entitled to injunctive relief requiring Defendant to (i) strengthen its data security protocols and procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit and identity monitoring to Plaintiff.**

## COUNT II: BREACH OF IMPLIED CONTRACT

**94. Plaintiff repeats and re-alleges each and every factual allegation contained in each of the previous paragraphs as if fully set forth herein.**

**95. Through its course of conduct, Defendant, Plaintiff entered into implied contracts for the provision of telecommunications services, as well as implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's Private Information.**

**96. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when Plaintiff signed up with AT&T for telecommunications services.**

**97. The valid and enforceable implied contracts to provide telecommunications services that Plaintiff entered into with Defendant include the promise to protect non-public Private Information given to Defendant or that Defendant creates on its own from disclosure.**

**98. When Plaintiff provided his Private Information to Defendant in exchange for telecommunications services, Plaintiff entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.**

**99. Defendant solicited Plaintiff to provide his Private Information as part of Defendant's regular business practices. Plaintiff accepted Defendant's offers and provided his Private Information to Defendant.**

**100. In entering into such implied contracts, Plaintiff reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.**

**101. Plaintiff who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to ensure adequate data security. Defendant failed to do so.**

**102. Under the implied contracts, Defendant promised and was obligated to: (a) provide telecommunications services to Plaintiff; and (b) protect Plaintiff's and his Private Information. In exchange, Plaintiff agreed to pay money for these services, and to turn over his Private Information.**

**103. Both the provision of telecommunication services and the protection of Plaintiff's Private Information were material aspects of these implied contracts.**

**104. The implied contracts for the provision of telecommunications services – contracts that include the contractual obligations to maintain the privacy of Plaintiff's Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.**

**105. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's Private Information.**

**106.** **Customers of telecommunications services value their privacy, the privacy of their dependents, and the ability to keep their PII associated with obtaining telecommunications services private. To customers such as Plaintiff, telecommunications services that do not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than the similar services that adhere to industry standard data security. Plaintiff would not have entrusted his Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or entrusted his Private Information to Defendant in the absence of its implied promise to adopt reasonable data security measures.**

**107.** **Plaintiff contractually agreed to provide his Private Information to Defendant, and paid for the provided telecommunications services in exchange for, amongst other things, both the provision of telecommunications services and the protection of his Private Information.**

**108.** **Plaintiff performed his obligations under the contract when he paid for AT&T's telecommunications services and provided his Private Information.**

**109.** **Defendant materially breached its contractual obligation to protect the non-public Private Information Defendant had gathered when the sensitive information was accessed by unauthorized personnel as part of the cyberattacks and "Data Breach".**

**110.** **Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Privacy Notice.**

**111.** **Defendant did not maintain the privacy of Plaintiff's Private Information as evidenced by its repeated unauthorized disclosures of Private Information to at least two**

**cybercriminal actors—ShinyHunters and MajorNelson. Specifically, Defendant did not comply with industry standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's Private Information, as set forth above.**

**112. The "Data Breach" was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.**

**113. As a result of Defendant's failure to fulfill the data security protections promised in his contract, Plaintiff did not receive the full benefit of the bargain, and instead received telecommunications services that were of a diminished value to that described in the contracts. Plaintiff therefore was damaged in an amount at least equal to the difference in the value of the telecommunications services with data security protection he paid for and the telecommunications services he received.**

**114. Had Defendant disclosed that it did not adhere to industry-standard security measures, neither the Plaintiff, nor any other reasonable person would have purchased telecommunications services from Defendant.**

**115. As a direct and proximate result of the Data Breach, Plaintiff has been harmed and has suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of his Private Information, the loss of control of his Private Information, the imminent risk of suffering additional damages in the future, disruption of their telecommunications services, out-of-pocket expenses, and the loss of the benefit of the bargain Plaintiff had struck with Defendant.**

**116. Plaintiff is entitled to compensatory, consequential and exemplary damages suffered as a result of the "Data Breach".**

**117.** **Plaintiff is also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; (iii) verify the adequacy of security measures implemented by Defendant's third-party processors of AT&T's Private Information; and (iv) provide adequate credit and identity monitoring to Plaintiff.**

## COUNT III: UNJUST ENRICHMENT

**118.** **Plaintiff repeats and re-alleges each and every factual allegation contained in each and every previous paragraph as if fully set forth herein.**

**119.** **Plaintiff conferred a monetary benefit on Defendant.**

**120.** **Specifically, Plaintiff purchased goods and services from Defendant and in so doing provided Defendant with his Private Information. In exchange, Plaintiff should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.**

**121.** **Defendant knew that Plaintiff conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff for business purposes.**

**122.** **The amount Plaintiff paid for goods and services were used, in part, to pay for the use of Defendant's network and the administrative costs of data management and security.**

**123.** **Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.**

**124.** **Defendant failed to secure Plaintiff's Private Information and, therefore, did not provide full compensation for the benefit Plaintiff provided.**

**125.** **Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.**

**126.** **If Plaintiff knew that Defendant had not reasonably secured his Private Information, Plaintiff would not have agreed to Defendant's services.**

**127.** **Plaintiff has no adequate remedy at law.**

**128.** **As a direct and proximate result of Defendant's conduct, Plaintiff has suffered and will continue to suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of his Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the "Data Breach", including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to his Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff.**

**129.** **As a direct and proximate result of Defendant's conduct, Plaintiff has**

**suffered and will continue to suffer other forms of injury and/or harm.**

**PLAINTIFF'S PRESENT AND FUTURE DAMAGES**

**130. To date, Defendant has done absolutely nothing to provide any relief for the damage Plaintiff has suffered as a result of the "Data Breach".**

**131. Plaintiff has been damaged by the compromise of his Private Information in the "Data Breach".**

**132. Plaintiff has continued to research the "Data Breach" and has learned that it involved 73 million AT&T customers' Private Information.**

**133. Plaintiff has since confirmed that his Private Information was indeed impacted in the "Data Breach" (Exhibit A) and that his Private Information is readily accessible via a search of the publicly available database containing AT&T customers' Private Information.**

**134. Plaintiff's Private Information was compromised as a direct and proximate result of the "Data Breach".**

**135. As a direct and proximate result of Defendant's conduct, Plaintiff has been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.**

**136. As a result of the "Data Breach", the Private Information of over 73 million AT&T customers, including Plaintiff, is available on the Internet for users, including criminals, to find, search through, and download.**

**137. As a direct and proximate result of Defendant's conduct, Plaintiff has been forced to expend time dealing with the effects of the "Data Breach".**

**138.** **Plaintiff faces substantial risk of out-of-pocket fraud losses such as loans opened in his name, medical services billed in his name, tax return fraud, utility bills opened in name, credit card fraud, and similar identity theft.**

**139.** **Plaintiff faces substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on his Private Information as potential fraudsters could use that information to target such schemes more effectively upon Plaintiff.**

**140.** **Plaintiff must now incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the "Data Breach".**

**141.** **Plaintiff has also suffered a loss of value of his Private Information when it was acquired by cyber thieves in the "Data Breach". Numerous courts have recognized the propriety of loss of value damages in related cases.**

**142.** **Plaintiff was also damaged via benefit-of-the-bargain damages. Plaintiff overpaid for a service that was intended to be accompanied by adequate data security, but was not. Part of the price Plaintiff paid to AT&T was intended to be used by AT&T to fund adequate security of Plaintiff's Private Information. Thus, Plaintiff did not get what he paid for.**

**143.** **Plaintiff has spent and will continue to spend significant amounts of time to monitor his financial accounts and records for misuse.**

**144.** **Indeed, AT&T has not yet provided any instructions to Plaintiff about all the time that he will need to spend monitor their own accounts, or about how to establish a security freeze on his credit report.**

**145. Plaintiff has suffered or will suffer actual injury as a direct result of the "Data Breach". Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to: Finding fraudulent charges; Canceling and reissuing credit and debit cards; Purchasing credit monitoring and identity theft prevention; Addressing their inability to withdraw funds linked to compromised accounts; Trips to banks and waiting in line to obtain funds held in limited accounts; Placing "freezes" and "alerts" with credit reporting agencies; Time on the phone with the bank to dispute fraudulent charges; Contacting other financial institutions and closing or modifying financial accounts; Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones; Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled, and; Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.**

**146. Moreover, Plaintiff has an interest in ensuring that his Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.**

**147. Furthermore, as a result of Defendant's conduct, Plaintiff is forced to live with the anxiety that his Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting him to**

**embarrassment and depriving him of any right to privacy whatsoever.**

**148. As a direct and proximate result of Defendant's actions and inactions, Plaintiff has suffered a loss of privacy and are at an imminent and increased risk of future harm.**

## PRAYER FOR RELIEF

**149. WHEREFORE, Plaintiff as described above, seeks the following relief:**

**150. Judgment in favor of Plaintiff awarding him appropriate monetary relief, including actual damages, statutory damages, exemplary damages, equitable relief, restitution, disgorgement, and statutory costs.**

**151. Judgment in favor of Plaintiff for exemplary damages as a result of Defendant's actions resulting in damages and harm to Plaintiff.**

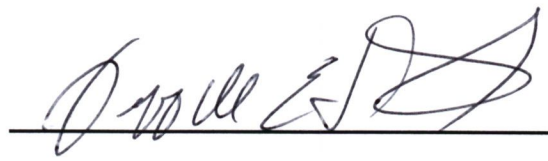
**152. A judgment in favor of Plaintiff awarding prejudgment and post-judgment interest and expenses as allowable by law; and**

**153. An award of such other and further relief as this Court may deem just and proper.**

## DEMAND FOR JURY TRIAL

**154. Plaintiff respectfully demands a jury trial as to all matters contained herein and so triable.**

**Respectfully Submitted,**



10-21-2024

**Jeff M Edwards** **Date**

***Pro Se***

**1406 Duster Cv**
**Cedar Park, Texas 78613**
**512-300-7555**
**JeffEdwards777@gmail.com**

AT&T

EXHIBIT

A

Jeff Edwards
1406 Duster Cv.
Cedar Park, TX 78613-5822

# NOTICE OF DATA BREACH

April 25, 2024

Hello,

At AT&T, we take the security of your data very seriously. We're writing to inform you that AT&T has determined that some of your personal information was compromised. To help protect your identity, we're offering you one year of complimentary credit monitoring, identity theft detection and resolution services provided by Experian's® IdentityWorks℠. **While this service is free, you must follow the enclosed instructions to enroll if you haven't already taken action based on our previous communication.**

**What happened?** On March 26, 2024, we determined that AT&T customer information was included in a dataset released on the dark web on March 17, 2024.

**What information was involved?** The information varied by individual and account, but may have included full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and AT&T passcode. To the best of our knowledge, personal financial information and call history were not included. Based on our investigation to date, the data appears to be from June 2019 or earlier.

**What is AT&T doing to help?** We're offering you the complimentary credit monitoring, identity theft detection and resolution services described above. We've also launched a robust investigation supported by internal and external cybersecurity experts, and we are regularly reviewing and updating the measures we take to protect your information.

**What can you do?**

- **Stay vigilant.** We recommend that you review the enclosed Information About Identity Theft Protection and encourage you to remain vigilant by monitoring your personal accounts and credit reports for any suspicious activity.
- **Watch out for suspicious calls or emails.** We also recommend that you remain alert for unsolicited communications seeking your personal information. You should be cautious about entering your username and password on links provided through emails, even if it looks like the company's website. The safest route is to go directly to the company's website to log in.

We apologize this has happened.

Please do not hesitate to call us at 866.346.0416 Monday through Friday, 8 a.m. to 9 p.m. CST, or visit att.com/accountsafety if you have questions regarding this matter.

Sincerely,

AT&T

**Experian's® IdentityWorks℠**

AT&T is providing you with an IdentityWorks℠ membership at no charge. After you complete registration, you'll have increased visibility into any possible fraudulent activity. You will also have an insurance policy of up to $1 million in coverage should you experience identity theft and an Identity Restoration team to guide you through the recovery process.

To activate your membership and start monitoring your personal information, please follow the steps below:

- **Enroll by August 30, 2024** (Your code will not work after this date.)
- **Go to** ExperianIDWorks.com/pluscreditlock and select 'Get Started'
- **Enter** your activation code: **KCZC5T3H7R**

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian's® IdentityWorks℠ online, please contact Experian's customer care team at 833.931.4853 by **August 30, 2024**. Be prepared to provide engagement number **(B119859)** as proof of eligibility for the identity restoration services provided by Experian.

**IdentityWorks℠ Includes:**

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms, and bulletin boards 24/7 to identify trading or selling of your personal information on the dark web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Credit Lock / Unlock:** This key feature provides you the ability to lock / unlock your Experian credit file.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian® IdentityWorks℠ membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please note that Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

## Information About Identity Theft Protection

### Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-866-349-5191
www.equifax.com

Experian®
P.O. Box 2002
Allen, TX 75013-9701
1-866-200-6020
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

You should remain vigilant for incidents of fraud or identity theft by reviewing account statements and monitoring free credit reports. When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information about you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

### Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax®
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
www.equifax.com/personal/credit-report-services

Experian®
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion®
P.O. Box 160
Woodlyn, PA 19094
1-800-916-8800
www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- Full name, with middle initial and any suffixes;
- Social Security number;
- Date of birth (month, day, and year);
- Current address and previous addresses for the past five (5) years;
- Proof of current address, such as a current utility bill or telephone bill;
- Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three business days after getting your request.

### Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts one year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax®
P.O. Box 105069
Atlanta, GA 30348-5069
1-800-525-6285
www.equifax.com/personal/credit-report- services/credit-fraud-alerts/

Experian®
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion®
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-alerts

**Federal Trade Commission and State Attorneys General Offices**

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state Attorney General and file a police report; this notice was not delayed by law enforcement. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338), to learn more about identity theft and the steps you can take to protect yourself and prevent such activity.

- Oregon residents are advised to report any suspected identity theft to law enforcement, including the FTC, and the Oregon Attorney General.
- North Carolina residents may also contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.
- Iowa residents are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.
- If you are a Maryland resident, you may contact the Maryland Office of the Attorney General at Consumer Protection Division Office, 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, https://www.marylandattorneygeneral.gov/Pages/contactus. aspx, 1-888-743-0023, or 410-528-8662 (consumer).
- District of Columbia residents may contact the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, 400 6th St. NW, Washington, D.C. 20001, https://oag.dc.gov/, (202) 442-9828 (consumer protection hotline).
- Rhode Island residents may contact the Office of the Attorney General, 150 South Main Street, Providence, RI 02930, (401) 274-4400.

**For New York Residents**

New York residents can also consider placing a Security Freeze on their credit reports. A Security Freeze prevents most potential creditors from viewing your credit reports, further protecting against the opening of unauthorized accounts. Please note that credit reporting agencies may charge a fee to place a Security Freeze. For more information on placing a security freeze on your credit reports, please review the New York Department of State Division of Consumer Protection website at https://dos.ny.gov/consumer-protection.

When you receive a credit report from a credit reporting agency, review the report carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. If you see anything that you do not understand or recognize, call the credit reporting agency at the telephone number on the report. You should also call your local police department and file a report of identity theft. Finally, you should make sure to keep a copy of the police report in case you need to provide it to creditors or credit reporting agencies when accessing or disputing inaccurate information.

Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant in reviewing your credit reports from the three major credit reporting agencies. You may obtain a free copy of your credit report once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228 or by completing an Annual Credit Request Form at: www.ftc.gov/bcp/menus/consumer/credit/rights.shtm and mailing to:

Annual Credit Report Request Service
P.O. Box 1025281
Atlanta, GA 30348-5283

You may report any incidents of suspected identity theft to law enforcement, including the FTC, your state Attorney General's office, or local law enforcement. For more information on identity theft, you can visit the following websites:

- New York Department of State Division of Consumer Protection: https://dos.ny.gov/consumer-protection; 1-800-697-1220
- NYS Attorney General at: https://ag.ny.gov/; 1-800-771-7755
- FTC at: www.ftc.gov/bcp/edu/microsites/idtheft/; https://www.identitytheft.gov/#/

AT&T

P.O. BOX 10758
San Bernardino, CA 92423-0758

RcvD 5/6/24

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE
**PAID**
AT&T

# Important information

379223 / 02 / C 977/0

Jeff Edwards
1406 Duster Cv.
Cedar Park, TX 78613-5822

ATTB 04/24

Gmail

Jeff Edwards <jeffe

EXHIBIT B

## Your Personal Data Breach Report

1 message

**F-Secure** <no-reply@f-secure.com>
To: jeffedwards777@gmail.com

Fri, Oct 18, 2024 at 3:58 PM

F-Secure

# Your data has been exposed

You have requested F-Secure's free report to see if your email address has been part of a data breach. Here's what we discovered:

**13 breach(es) that contain your personal information:**

| Breached Service | Exposed data |
|---|---|
| 2021 AT&T Subscriber Data<br>03/2024 | Street address , City , Date of birth , Email address , Full name , Phone number , Postal code , Social security number , State |
| zeeroq.com<br>02/2024 | Email address , Password |
| USA Valid Emails<br>08/2023 | City , Country , Email address , First name , Full name , Last name , Postal code , State |
| Online Digital<br>06/2023 | Country , Email address , First name , Full name , Last name |

EXHIBIT
C

**UNITED STATES JUDICIAL PANEL**
**on**
**MULTIDISTRICT LITIGATION**



**IN RE: AT&T INC. CUSTOMER DATA SECURITY BREACH LITIGATION**

MDL No. 3114

**TRANSFER ORDER**

**Before the Panel:*** Plaintiffs in the actions listed on Schedule A and Schedule B move under Panel Rule 7.1 to vacate the orders conditionally transferring the actions to MDL No. 3114.[1] Defendants AT&T Inc. and AT&T Mobility LLC oppose the motions and support transfer.

After considering the argument of counsel, we find that the actions involve common questions of fact with the actions transferred to MDL No. 3114, and that transfer under 28 U.S.C. § 1407 will serve the convenience of the parties and witnesses and promote the just and efficient conduct of the litigation. In our order establishing this MDL, we held that centralization was warranted for actions concerning "an alleged data security breach announced by AT&T in March 2024 concerning the personal information of over 70 million former and current AT&T customers released on the dark web."[2] *See In re AT&T Inc. Customer Data Sec. Breach Litig.*, __ F. Supp. 3d __, 2024 WL 2884429 (J.P.M.L. June 5, 2024). The actions concern the AT&T data breach announced in March 2024 and share common factual questions with the actions in the MDL.

In opposition to transfer, the *pro se* plaintiffs in *Phillips* argue that (1) there are "*also* questions of fact that are uncommon" to the MDL, and (2) transfer to a distant forum will be

* Judge Karen K. Caldwell and Judge David C. Norton did not participate in the decision of this matter.

[1] The Schedule A actions assert claims concerning the data breach at issue in MDL No. 3114 and were the subject of conditional transfer orders providing for transfer of the actions in their entirety. *See* CTO-2, CTO-3, and CTO-6. The Schedule B actions assert claims concerning both the data breach and an allegedly unlawful monthly administrative fee unrelated to the data breach claims. For the Schedule B actions, the CTO provided for transfer of the actions with simultaneous separation and remand of the claims challenging the administrative fee to the transferor court. *See* CTO-7. All parties to the Schedule B actions agree that exclusion of the administrative fee claims from the MDL is appropriate and do not challenge that part of the CTO.

[2] The personal information allegedly compromised by the breach was from a 2019 data set and included customer names, addresses, phone numbers, social security numbers, dates of birth, AT&T account numbers, and passcodes. *See In re AT&T Inc. Customer Data Sec. Breach Litig.*, 2024 WL 2884429, at *1 n.2.

inconvenient for their action. These objections are unpersuasive. First, plaintiffs do not indicate what the purported "uncommon" questions are. Assuming that their case does raise some case-specific factual questions (e.g., their individual relationship with AT&T), transfer remains warranted. Section 1407 does not require a complete identity of common factual issues or parties when the actions arise from a common factual core. *See In re Valsartan Prods. Liab. Litig.*, 433 F. Supp. 3d 1349, 1352 (J.P.M.L. 2019). Additionally, the alleged inconvenience of transfer does not weigh against transfer. The Panel looks to "the overall convenience of the parties and witnesses in the litigation as a whole, not just those of a single plaintiff or defendant in isolation." *See In re Watson Fentanyl Patch Prods. Liab. Litig.*, 883 F. Supp. 2d 1350, 1351-52 (J.P.M.L. 2012). Moreover, because transfer is for pretrial proceedings only, there likely will be no need for plaintiffs to travel to the transferee forum.

Plaintiffs in the remaining seven actions principally argue that their actions were improperly removed and that the interest of efficiency is best served by allowing the transferor courts to decide the issues presented in their pending or anticipated motions for remand to state court. The Panel consistently has held, however, that jurisdictional objections do not present an impediment to transfer. *See, e.g., In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 170 F. Supp. 2d 1346, 1347 (J.P.M.L. 2001) (explaining that "remand motions can be presented to and decided by the transferee judge" and transferor courts wishing to rule on such motions generally "have adequate time to do so").

Plaintiffs in five actions (*Caruso, Surowiec, Young, Varela*, and *Quick*) also seek an order from the Panel remanding their actions to state court. The Panel does not have the authority to order remand of actions to state court. *See In re Ford Motor Co. DPS6 Powershift Transmission Prods. Liab. Litig.*, 289 F. Supp. 3d 1350, 1352 (J.P.M.L. 2018) ("Section 1407 does not empower the MDL Panel to decide questions going to the jurisdiction or the merits of a case, including issues relating to a motion to remand.").

IT IS THEREFORE ORDERED that the actions listed on Schedule A and Schedule B are transferred to the Northern District of Texas and, with the consent of that court, assigned to the Honorable Ada E. Brown for coordinated or consolidated pretrial proceedings.

IT IS FURTHER ORDERED that the administrative fee claims in the actions listed on Schedule B are simultaneously separated and remanded to the Southern District of Florida.

PANEL ON MULTIDISTRICT LITIGATION

Nathaniel M. Gorton
Acting Chair

Matthew F. Kennelly
Dale A. Kimball
Roger T. Benitez
Madeline Cox Arleo

**IN RE: AT&T INC. CUSTOMER DATA SECURITY BREACH LITIGATION**

MDL No. 3114

**SCHEDULE A**

Middle District of Florida

RASLAVICH v. AT&T INC., C.A. No. 8:24−01422

Southern District of Florida

CARUSO v. AT&T MOBILITY LLC, C.A. No. 1:24−22597
PHILLIPS, ET AL. v. AT&T MOBILITY LLC, ET AL., C.A. No. 9:24−80700

Western District of Texas

EDWARDS v. AT&T INC., C.A. No. 1:24−00753

**IN RE: AT&T INC. CUSTOMER DATA SECURITY BREACH LITIGATION**

MDL No. 3114

**SCHEDULE B**

Southern District of Florida

SUROWIEC v. AT&T MOBILITY LLC, C.A. No. 1:24−22619
YOUNG v. AT&T MOBILITY LLC, C.A. No. 1:24−22625
VARELA v. AT&T MOBILITY LLC, C.A. No. 1:24−22666
QUICK v. AT&T MOBILITY LLC, C.A. No. 1:24−22682

Securing today and tomorrow

EXHIBIT
D

# Identity Theft and Your Social Security Number

SSA.gov

Identity theft is one of the fastest growing crimes in America. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.

Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

## Your number is confidential

The Social Security Administration protects your Social Security number and keeps your records confidential. We don't give your number to anyone, except when authorized by law. You should be careful about sharing your number, even when you're asked for it. You should ask why your number is needed, how it'll be used, and what will happen if you refuse. The answers to these questions can help you decide if you want to give out your Social Security number.

## How might someone steal your number?

Identity thieves get your personal information by:

- Stealing wallets, purses, and your mail (bank and credit card statements, pre-approved credit offers, new checks, and tax information).
- Stealing personal information you provide to an unsecured site online, from business or personnel records at work, and personal information in your home.
- Rummaging through your trash, the trash of businesses, and public trash dumps for personal data.
- Buying personal information from "inside" sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services, or credit.
- Posing by phone or email as someone who legitimately needs information about you, such as employers, landlords, or government agencies.

## Be careful with your Social Security card and number

When you start a job, make sure your employer has your correct Social Security number so your records are correct. Provide your Social Security number to your financial institution(s) for

tax reporting purposes. Keep your card and any other document that shows your Social Security number in a safe place. DO NOT routinely carry your card or other documents that display your number.

## What if you think someone is using your number?

Sometimes more than one person uses the same Social Security number, either on purpose or by accident. If you suspect someone is using your number for work purposes, you should contact us to report the problem. We'll review your earnings with you to ensure our records are correct.

You also may review earnings posted to your record on your *Social Security Statement*. The *Statement* is available online to workers age 18 and older. To get your *Statement*, go to ***www.ssa.gov/myaccount*** and create an account.

## What if an identity thief is creating credit problems for you?

If someone has misused your Social Security number or other personal information to create credit or other problems for you, Social Security can't resolve these problems. But there are several things you should do.

Visit ***IdentityTheft.gov*** to report identity theft and get a recovery plan. ***IdentityTheft.gov*** guides you through each step of the recovery process. It's a one-stop resource managed by the Federal Trade Commission, the nation's consumer protection agency. You can also call **1-877-IDTHEFT** (**1-877-438-4338**); TTY **1-866-653-4261**.

You may want to contact the Internal Revenue Service (IRS). An identity thief also might use your Social Security number to file a tax return to receive your refund. If you're eligible for a refund, a thief could file a tax return before you do and get your refund. Then, when you do file, the IRS will think you already received your refund. If your Social Security number is stolen, another person may use it to get a job. That person's employer would report earned income to the IRS using your Social Security number. This will make it appear that you didn't report all of your income on your tax return. If you think you may have tax issues because someone has stolen your identity, go to ***www.irs.gov/uac/Identity-Protection*** or call **1-800-908-4490**.

Also, you should file an online complaint with the Internet Crime Complaint Center (IC3) at ***www.ic3.gov***.

The IC3 gives victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations.

IC3 sends every complaint to one or more law enforcement or regulatory agencies with jurisdiction.

IC3's mission is to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cybercrime. The IC3 serves the broader law enforcement community that combats internet crime. This includes federal, state, local, and international agencies.

The IC3 reflects a partnership between the Federal Bureau of Investigation, the National White Collar Crime Center, and the Bureau of Justice Assistance.

You should also monitor your credit report periodically. You can get free credit reports online at ***www.annualcreditreport.com***.

## Should you get a new Social Security number?

If you've done all you can to fix the problems resulting from misuse of your Social Security number, and someone is still using your number, we may assign you a new number.

You can't get a new Social Security number:

- If your Social Security card is lost or stolen, but there's no evidence that someone is using your number.
- To avoid the consequences of filing for bankruptcy.

- If you intend to avoid the law or any legal responsibility.

If you decide to apply for a new number, you'll need to prove your identity, age, and U.S. citizenship or immigration status. For more information, ask for *Your Social Security Number and Card* (Publication Number 05-10002). You'll also need to provide evidence that you're having ongoing problems because of the misuse.

Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security number, you shouldn't use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.

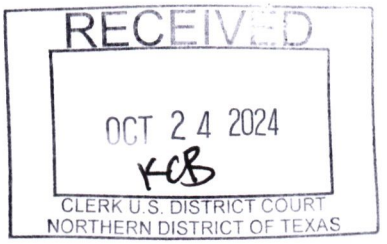
## Contacting Social Security

The most convenient way to do business with us from anywhere, on any device, is to visit ***www.ssa.gov***. There are several things you can do online: apply for benefits; get useful information; find publications; and get answers to frequently asked questions.

Or, you can call us toll-free at **1-800-772-1213** or at **1-800-325-0778** (TTY) if you're deaf or hard of hearing. We can answer your call from 7 a.m. to 7 p.m., weekdays. You can also use our automated services via telephone, 24 hours a day. We look forward to serving you.

**Social Security Administration**
Publication No. 05-10064
July 2021 (June 2018 edition may be used)
Identity Theft and Your Social Security Number
Produced and published at U.S. taxpayer expense

**Jeff M Edwards**
1406 Duster Cv
Cedar Park, TX 78613




October 21, 2024

USPS Priority Mail ~ Delivery Confirmation Tracking

District Clerk
United States District Court
Northern District of Texas
1100 Commerce St
Room 1542
Dallas, TX 75242

Re: Edwards vs AT&T Inc – Case No. 3:24-cv-02543-E – MDL 3:24-md-03114

To The District Clerk,

Please see attached "Plaintiff's Amended Complaint" for which I am requesting to be filed in my behalf for the above-named case.

Pursuant to Rule 4 of the Federal Rules of Civil Procedure, I will be sending, concurrent with this filing, a Waiver of the Service of Summons to Defendant's counsel of record.

If you have any questions or further instructions, please contact me directly via email or by phone.

Regards,

Jeff M Edwards

Pro Se

Email: JeffEdwards777@gmail.com

Phone: (512) 300-7555

Retail

U.S. POSTAGE PAID
USPS Ground Advtg
CEDAR PARK, TX 78613
OCT 21, 2024

75242

$7.05

RDC 01 0 Lb 9.60 Oz S2323Y501264-7

From: Jeff M Edwards
1406 Duster Cv
Cedar Park, TX 78613

RECEIVED-1
OCT 24 2024
MAILROOM

To: District Clerk
United States District Court
Northern District of Texas
1100 Commerce St
Room 1452
Dallas, TX 75242

USPS TRACKING® #

9500 1140 0922 4295 9759 32